AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

CYBERSPACE: A LAWLESS WORLD

by

Pauline N. Harke, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Fred Stone

Maxwell Air Force Base, Alabama

February 2016

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Contents

Acknowledgements

I would like to thank my classmates for all their valuable feedback during the development of this research paper. I would especially like to thank my instructor and advisor, Dr. Fred Stone, whose guidance and advice made this paper possible. Finally, I would also like to thank my friends and family for their support as I worked on this paper, especially my husband, whose patience and assumption of all household responsibilities, allowed me to focus completely on the accomplishment of this research paper.

Abstract

Cyberattacks in the last decade have severely crippled businesses and compromised individual and national security. Any organization with a stake in cyberspace is vulnerable to attack, espionage, or criminal activity. Despite a reported 782% increase in cyber incidents over a six year period, many cyber attackers and cyber criminals do not face any repercussions for their actions. This research paper addresses the lack of accountability in cyberspace by examining three potential frameworks that can provide operational direction for an approach to accountability that expands on the strategies outlined in the 2015 National Security Strategy and the 2011 International Strategy for Cyberspace. The alternatives were analyzed against a specific set of criteria - whether they resolve the major barriers to regulation that have persisted thus far, whether they are practical, whether they provide for a consistent approach to accountability, and whether they will serve as a significant deterrent to potential cyber attackers and cyber criminals. The results of this research found that the creation of an international body for cyberspace governance would best resolve some of the major barriers to regulation and serve to aid in the establishment of a system of accountability. The advantage of this collaborative forum is that it has the ability to expedite the standardization of laws and language throughout the international community, and ultimately aid in the creation of one strategic agenda for the development of shared norms for conduct in the virtual world.

Introduction

Cyberspace has added an unprecedented level of convenience to operations in industries across the globe. In the United States military, the warfighter is presented with real-time information, and the lines between the levels of warfare have blurred as high level commanders can access the battlefield through advanced command and control systems. Business transactions now occur without any reliance on physical paperwork. The added level of convenience, however, has introduced a number of vulnerabilities that the Department of Defense has not been able to mitigate. Cyberattacks in the last decade have crippled businesses and compromised individual and national security. Between 2006 and 2012, the number of cyber incidents reported per year in the United States rose from 5,503 to 48,562, a 782% increase.[1] The economic impact is estimated to be in the hundreds of billions of dollars lost worldwide.[2] Yet, according to the Federal Bureau of Investigation statistics in 2010, only six convictions were made to prosecute cyber criminals as the United States does not have jurisdiction over criminals residing in other countries and domestic law enforcement is limited by state borders.[3] This disparity suggests a lack of governable cyber laws that hold cyber attackers and cyber criminals accountable.

With the ever increasing cyberattacks, this research paper examines how accountability can be established for crimes and attacks taking place in cyberspace. To help answer this question, the problem/solution framework was used to first explain the problem and identify the major barriers to regulation. While a number of barriers make the development of effective

[1] Gregory C. Wilshusen, *Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges*, GAO-13-462T (Washington D.C.: U.S. Government Accountability Office, 2013), 6.
[2] Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime, staff study, June 2014.
[3] Internet Crime Complaint Center, "2010 Internet Crime Report," (National White Collar Crime Center, 2011), 6.

cyber regulation difficult, this research paper will discuss the four most common barriers, which include differing cyber laws in many countries, jurisdictional issues, insufficient standardization of cyber language, and foreign relationships. Overcoming these barriers would aid in the effort to establish accountability for cyber violations. The research paper will then discuss three potential solutions that seek to resolve the accountability issue. To analyze the potential solutions, a specific set of criteria will be established and discussed. Each solution will then be analyzed against this criteria to evaluate how well the solution resolves the issue. The results of this research will inform military and Department of Defense leaders in the hope that their influence and further research sets a defined approach for the development of an effective system of accountability in cyberspace.

Strategic Guidance

The 2010 National Security Strategy (NSS) introduced the threats and vulnerabilities that cyberspace poses and promoted the need for increased cybersecurity.[4] It was followed by the landmark 2011 International Strategy for Cyberspace, which expanded on the goals set forth in the 2010 NSS.[5] This document was the first comprehensive strategic document the United States produced that addressed cyberspace concerns. In it, the President recognized the challenges that cyberspace poses as the problems transcend national borders.[6] He called for global cooperation, grounded in principle, to ultimately preserve the fundamental freedoms, privacy, and free flow of information for all citizens of the world.[7]

[4] Barack H. Obama, *National Security Strategy*, (Washington, D.C.: Government Printing Office, 2010), 1-52.
[5] Barack H. Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,* (Washington, D.C.: The White House, May 2011), 1-25.
[6] Ibid, 4.
[7] Ibid, 5.

Each year, the United States Intelligence Community produces the Worldwide Threat Assessment that lists the top U.S. security concerns. In the 2013 assessment, cyber terrorism and cyber espionage passed terrorism as the top security concern.[8] As a result, cyber security became the focus as the Air Force's Cyber Command led the defensive effort to centralize control by reducing the number of network entry points.[9] As boosting cyber security efforts improves the defensive posture of military networks, it is only addressing part of the problem. Cyber attribution has grown into a multi-billion dollar industry as a plethora of private companies compete to trace the origins of hacker activity through fiber-optic cables and web domains. Despite the improved cyber forensics capabilities, the majority of cyber attackers remain free of prosecution. Lt. Gen Keith Alexander, former commander of United States Cyber Command, reported that military networks receive hundreds of thousands of probes a day.[10] Probes that allow attackers to identify weaknesses and vulnerabilities in military networks lead to the creation of lethal viruses that can halt operations or present major national security risks.

Up until 2015, the NSS had addressed cyber issues, but had focused mainly on the defense of the networks. In the 2015 version of the document, the published intent to prosecute cyber criminals for their illegal activity is a significant step toward promoting accountability in cyberspace.[11] In addition, the 2015 NSS publicly recognized that managing the security of the Internet is a shared responsibility between states and commits to offer assistance to other

[8] James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, (Washington DC: Senate Select Committee on Intelligence, 2013), 1-2.
[9] Gen William L. Shelton, (Speech, AFCEA Cyberspace Symposium, Colorado Springs, CO, 6 Feb 2013).
[10] Gen Keith Alexander (Former Commander, U.S. Cyber Command), "U.S. Cybersecurity Policy and the Role of U.S. Cybercom," Discussion moderated by James Lewis, 3 June 2010, Center for Strategic and International Studies, Washington D.C.
[11] Barack H. Obama, *National Security Strategy*, (Washington, D.C.: Government Printing Office, 2015), 13.

countries in the development of laws that enable strong action against threats that originate from their infrastructure.[12]

The Private Sector

The national security risks extend beyond military networks. The economy, safety and health of U.S. citizens are linked through a networked infrastructure in which 80% of this critical infrastructure is operated or owned by the private sector.[13] These commercial networks are vital to military operations with over 90% of the military's energy operated by the private sector and more than 80% of military logistics relying on private companies for their transportation needs.[14] Therefore, protecting privately owned and operated infrastructure is of vital importance to national security. Critical infrastructure consists of "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[15] A physical attack on any of this key infrastructure would be considered an act of war and would most likely be followed by a military response. Yet, a virtual attack of this level still does not seem to yield such a response. A prime example that illustrates the lack of accountability in cyberspace comes from the 2013 series of distributed denial of service attacks by the activist group, Cyber Fighters of Izz ad-din Al Qassam. Their attack affected many key parts of the telecommunications and financial services infrastructure that were, according to then House Intelligence Committee Chairman, Mike

[12] Ibid.
[13] William Waddell, David Smith, James Shufelt, and Jeffrey Caton, United States Army War College, Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace, CSL Study 1-11, Center for Strategic Leadership, March 2011, 16.
[14] Alexander, "U.S. Cybersecurity Policy and the Role of U.S. Cybercom."
[15] Department of Homeland Security, "Critical Infrastructure Sectors," http://www.dhs.gov/critical-infrastructure-sectors.

Rogers, "stressed to a dangerous level."[16] Despite the impact of the attack and members of congressional intelligence committees claiming that the attacks were sponsored by Iran, no further action was taken to hold the attackers or Iran accountable. Effective regulation that holds cyber attackers accountable for their actions is necessary in the effort to deter future attacks and secure the nation's borders. The current lack of effective regulation points to some major hurdles unique to cyberspace that still need to be tackled in order for these regulations to succeed.

Shared Norms

The idea of regulating cyberspace is not a new idea. Since the introduction of the internet, many people have recognized a need for established regulations to maintain freedom and security in cyberspace. The Council of Europe's Convention on Cybercrime was developed in 2001 and is the only treaty that seeks to foster international cooperation on the issue of cyber legislation. Currently, 49 countries are signatories to the convention and 42 of these—including the United States—have ratified it.[17] The Convention requires signatories address four categories of computer-related crimes in their domestic laws: (1) security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability, (2) fraud and forgery, (3) child pornography, and (4) copyright infringements.[18] The convention also requires signatories to establish domestic procedures for detecting, investigating, and prosecuting computer crimes, as well as collecting electronic evidence of any

[16] Joseph Menn, "Cyber Attacks Against Banks More Severe Than Most Realize," Reuters, 18 May 2013, http://www.reuters.com/article/us-cyber-summit-banks-idUSBRE94G0ZP20130518.
[17] Council of Europe, "Convention on Cybercrime: Chart of signatures and ratifications of Treaty 185," Council of Europe, updated 1/26/2016, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.
[18] Kristin Archick, "Cybercrime: The Council of Europe Convention," Order Code RS21208, (Washington, DC: Congressional Research Service, 2004), CRS-2.

criminal offense.[19] Finally, it requires that signatories engage in international cooperation "to the widest extent possible."[20] While this treaty is a major milestone in the evolution of cyber legislation, the number of signatories to date represents only a fraction of the world's population. Major countries found to be responsible for hacking such as Russia and China have not signed it, nor have the majority of African countries. In addition, the Convention addresses cybercrimes but does not specifically address the higher national security threat of cyberterrorism. While the creation of the Convention was a positive step toward international collaboration, some believe its scope must be more far-reaching to create a lasting impact on cyberspace governance.[21]

Ultimately, international cyber law development is dependent on the promotion of shared norms. To do so, it will be necessary for the international community to embrace the principles set forth in the 2011 International Strategy for Cyberspace, which acknowledges that cyberspace contains unique aspects that will need to be addressed, but asserts that "long-standing international norms guiding State behavior – in times of peace and conflict – also apply in cyberspace".[22] The world today is connected via the Internet in all industries. There is no guarantee that the effects of a cyberattack on one nation will be isolated within its physical boundaries. The Talinn Manual is the most recent and comprehensive document that seeks to outline the law governing cyber warfare on a domestic and international scale.[23] It was created in 2009 by an independent international group of experts under the sponsorship of the NATO Cooperative Cyber Defense Centre of Excellence. While the manual is not considered an official

[19] Ibid.
[20] Council of Europe, *European Treaty Series - No. 185*, Convention on Cybercrime, 2001, Budapest, 23.XI.2001, 12.
[21] Krishna Prasad, "Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework," (paper presented at the 3rd Australian Counter Terrorism Conference, Perth, Australia, December 2013), 9-14.
[22] 2011 International Strategy for Cyberspace, 9.
[23] NATO Cooperative Cyber Defence Centre of Excellence, *Talinn Manual on the International Law Applicable to Cyber Warfare*, 2013.

document, it can provide a framework for the development of official legislation and supports the idea that existing legal frameworks can be applied in cyberspace as set forth in the U.S. International Strategy for Cyberspace.

Barriers to Regulation

The latest strategic guidance points to a desire to hold cyber attackers and cyber criminals accountable in an effort to curb the alarming increase in cyber incidents. The evidence presented thus far suggests a causative relationship between the lack of cyber regulation and the prevalence of cyber incidents in the United States. If the United States continues to maintain the same level of response to cyber incidents, the number of incidents will likely increase. Despite the increase, cyber law development has stalled, and the reason lies in a number of barriers that prevent the establishment of regulation.[24] Resolving these barriers will help to ensure that cyber laws are clear, consistent, and effective.

Standardization of Cyber Language

One critical uncertainty revolves around the lack of standardized cyber language. A number of terms are used when referring to cyber incidents. The terms cybercrime, cyber espionage, cyberterrorism, cyberattack, and cyber war are the most often used, and are often used interchangeably. This is mainly because there are not universally accepted definitions of what each term means and what activities fall under the umbrella of each type of incident. This leads many down a dangerous path as overuse of the term cyber war or information warfare when referring to cybercrime tends to sensationalize certain cybercrimes that may be threats to public

[24] Finklea, Kristin M., *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Concerning U.S. Law Enforcement*, CRS Report for Congress R41927 (Washington DC: Congressional Research Service, 2013), 1-38.

security but not necessarily threats to national security.[25] Many agencies and organizations have their own general ideas of what constitutes each type of incident, but without an agreed upon definition of each term, lines are often blurred or overlap. The lack of universally accepted terms has contributed to the problem of no single agency being designated as lead investigative agency for combating each of these types of cyber incidents. For example, the Federal Bureau of Investigation, the U.S. Secret Service, and others, all investigate cybercrimes, but none are considered the lead agency.[26] Without a universally accepted definition detailing the activities that constitute a cybercrime, gaps in investigation or duplication of effort ensues. Defining cyber terms is important because it will allow the government to exercise the principle of proportionality for the creation of laws, jurisdictional boundaries, and strategies appropriate for each type of incident. This can then be followed by the development of viable consequences for violators to be investigated and prosecuted at the appropriate level of government by clearly defined lead agencies.

On an international scale, these terms are also not agreed upon. While definitions are similar, small nuances within each countries' definitions can have different legal implications within each countries' judicial system. For example, the United States defines a cyberattack as "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."[27] New Zealand defines cyberattack as "an attempt to undermine or compromise

[25] David L. Speer, "Redefining Borders: The Challenges of Cybercrime," Crime, Law and Social Change 34, no. 3 (October 2000), 260.
[26] Finklea, *Interplay of Borders*, 7.
[27] NATO Cooperative Cyber Defense Centre of Excellence, "Cyber Definitions," https://ccdcoe.org/cyber-definitions.html

the function of a computer-based system, access information, or attempt to track the online movements of individuals without their permission."[28] Austria defines cyberattack as "an attack through IT in cyberspace, which is directed against one or several IT system(s). Its aim is to undermine the objectives of ICT security protection (confidentiality, integrity and availability) partly or totally."[29] Many of the definitions remain vague, leading to confusion on the part of the international community as to what type of attack falls within currently accepted jus ad bellum (just for war) clauses. The current challenge presented is the determination on whether defining cyber terminology should remain a domestic challenge for every country, or if the issue requires more of a global focus that seeks to create internationally accepted definitions of these terms for worldwide standardization of cyber law.

Jurisdictional Issues

While defining the various cyber terms is necessary for the development of effective cyber regulation, an even larger problem presents itself in the enforcement of these regulations. Domestic and international cyber laws vary from state to state and country to country. The majority of cyber incidents are carried out by an attacker or criminal residing in another country.[30] Jurisdictional issues then come into play, which gives rise to the need for extradition treaties. Since the United States does not have extradition treaties set up with many countries, cyber attackers and cyber criminals avoid prosecution. A potential cyber attacker is simply tasked with researching the countries with relaxed or non-existent cyber laws that also do not maintain extradition treaties with the countries they are attacking. Ensuring that their attacks

[28] Ibid.
[29] Ibid.
[30] United States Senate, *Investigating and Prosecuting 21st Century Cyber Threats: Hearings before the Subcommittee on Crime, Terrorism, Homeland Security and Investigations*, 113th Cong., 1st sess., 2013, 30.

originate within the borders of one of these countries allows perpetrators to freely initiate attacks or crimes without the fear of prosecution.

The 2011 take down of the Estonian-based criminal operation, Rove Digital, is an example of how global cooperation and established extradition treaties can lead to the successful prosecution of cyber criminals. Rove Digital was a highly profitable Internet fraud scheme involving millions of compromised computers located in over 100 countries. While the complex coordination effort, which involved a number of private and public sector organizations from various countries, has been applauded, the operation primarily owes its success to the ratified Multi-lateral Assistance Treaty Estonia had with the United States. This treaty was the driving force for the successful extradition of six Estonians to face trial in the United States, the last of which was brought to a close in July 2015 with the group's founder, Vladamir Tsastsin, pleading guilty to all charges.[31] Unfortunately, the situation with Estonia is an exception.

Varying Degrees of Cyber Legislation

Extradition treaties are not always necessary as long as the cyber attacker is held accountable within their residing country. However, many countries do not even have established cyber laws, thereby letting the cyber attacker remain free of prosecution and free to initiate more cyber incidents. Differing cyber laws amongst nations, such as those relating to privacy, also impede evidence collection in transnational investigations.[32] One of the most notable examples that opened up public discussion on inconsistent cyber laws was the "I Love You" or "Love Bug" virus that caused widespread damage as it swept through various

[31] John Garris, *There's No Going It Alone: Disrupting Major Crime Rings (A Case Study)*, (Bethesda, MD: SANS Institute, 2015), 13.
[32] *United States Faces Challenges in Addressing Global Cybersecurity and Governance*, Report to Congressional Requesters, GAO-10-606 (Washington DC: U.S. Government Accountability Office, July 2010), 43.

organizations in the United States and across the globe in 2000. This virus originated in the Philippines and authorities were able to successfully identify the creator. While the perpetrator was arrested, he was not charged with a crime because Philippine law at the time was not sufficient in addressing hacking and computer crimes.[33] The Philippine Congress subsequently passed a law specifically dealing with computer-related crimes, but at that point, the damage was done. This example highlights how important it is for countries to be proactive in initiating their own cyber legislation rather than waiting until a devastating attack occurs from within their borders to do so. Even within the United States, state laws vary and the current cyber threat landscape requires the nation to move beyond the patchwork of state laws pertaining to cyberspace by standardizing them into one federal statute.

Many countries lack sufficient legislation because they currently have little or no vested interest in creating them due to the minimal level in which they are impacted by cyber incidents. According to the FBI Internet Crime Complaint Center's 2014 Internet Crime Report, 91.54% of all cybercrime victim complainants came from the United States.[34] This statistic reveals that the United States has the greatest stake in the creation of effective cyber regulation. The example of the "Love Bug" virus gives much insight into the mindset of other countries. While there is a growing list of countries that now have, at the very least, a partially developed set of cyber laws, many states may not feel compelled to act due to the perceived lack of threat to its citizens and its borders. However, the "Love Bug" virus, and many subsequent viruses that have been released since then, reveal how quickly a virus can spread beyond the borders of the intended recipient country to wreak havoc worldwide.

[33] Finklea, *Interplay of Borders*, 11.
[34] Internet Crime Complaint Center, "2014 Internet Crime Report," (National White Collar Crime Center, 2014), 22.

Foreign Relationships

Foreign relationships further complicate the issue of cyberspace accountability. The United States has remained dedicated to maintaining stability in various regions of the world and fostering cooperative relationships with other nations. With the emergence of cyberspace, policy makers appear to struggle with balancing the development of strong relationships with these nations while also developing appropriate responses to cyber incidents, particularly in the case of state-sponsored cyber incidents. For example, the relationship between the United States and China has always been a fickle one peppered with varying degrees of distrust. Despite tensions, China has emerged as a valuable trade partner, becoming the second-largest U.S. trading partner (after Canada), the third-largest U.S. export market (after Canada and Mexico), and the largest source of U.S. imports.[35] While collaborative efforts in recent years have improved on many fronts, China has also become the source of roughly 70% of cyber thefts on intellectual property (IP) in the United States, and the world's largest source of IP theft.[36] The information accessed has included state secrets, weapons technology, business intellectual property, corporate negotiating strategies, personal files, and communications of high ranking and notable individuals.[37] President Obama has said theft of intellectual property is "one of the most serious economic and national security challenges we face," and Gen Alexander has called it "the greatest transfer of wealth in history."[38] The losses equate to billions of dollars and millions of jobs for American companies and citizens. Despite the staggering numbers, America's response

[35] Wayne M. Morrison, *China-U.S. Trade Issues*, CRS Report for Congress RL33536 (Washington DC: Congressional Research Service, 2015), 2.
[36] The IP Commission, *The Report of the Commission on the Theft of American Intellectual Property*, (The National Bureau of Asian Research, May 2013), 2-4.
[37] Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations*, (Washington, D.C.: The Brookings Institution, February 2012), 3.
[38] Ibid, 2-4.

has been limited to reprimands and talks with foreign leaders on the development of stronger intellectual property rights regimes.[39] One likely reason for such a response lies in the fact that taking a harsher stance toward Chinese cyber espionage threatens to disrupt the strong trade relationship between the United States and China. The September 2015 agreement between Chinese President Xi and President Obama, that announced that neither country would willingly conduct or knowingly support cyber-enabled theft of intellectual property,[40] sounded promising. However, on the tails of this agreement, U.S. counterintelligence chief, Bill Evanina, has stated that in regards to Chinese cyber intrusions, he had seen "no indication…that anything has changed."[41] An alternative solution to improve accountability in cyberspace must strike the delicate balance between being effective at addressing the issues of foreign IP theft and state-sponsored cyber intrusions while still preserving and promoting cooperative relationships with these international partners.

Criteria for Evaluation

The results of the analysis will determine the recommended path for the way ahead. First, it will be important for the alternative to resolve as many of the major barriers to regulation as possible. Inconsistent definition of cyber terms, jurisdictional and extradition issues, varying degrees of cyber legislation, and balancing foreign relationships have shown to be the biggest hurdles to overcome in the progression of cyber legislation. While a variety of other issues exist,

[39] Ibid, 10.
[40] Morrison, China-U.S. Trade Issues, 42.
[41] Mark Hosenball, "U.S. counterintelligence chief skeptical China has curbed spying on U.S.," Reuters, 18 November 2015, http://www.reuters.com/article/us-usa-cybersecurity-idUSKCN0T72XG20151119.

tackling these four barriers will significantly ease the path toward the establishment of regulation.

The second criteria will evaluate whether the alternative is practical. There are countless potential solutions to the problem of accountability in cyberspace. While many solutions may sound plausible when viewed independently of external factors, they may not be practical when applied to the complex arena of international politics. Since cyberspace is a man-made environment that is grounded in hardware and code-based protocols, the technical aspect of the alternative must also be reasonable based on current knowledge of technological capabilities. Ultimately, the alternative must pass the litmus test of whether it is a reasonable solution.

The third criteria examines whether the alternative provides for a consistent approach for holding cyber attackers and cyber criminals accountable. The current situation does not provide consistency since some perpetrators are prosecuted, while many are not. An attack or crime in the physical world is almost always followed up with an investigation or some form of a consequence. The inconsistency regarding consequences in cyberspace is a likely reason why so many perpetrators feel free to carry out attacks and crimes in the virtual environment.

Finally, the alternative must serve as a significant deterrent. The ultimate goal is to curb the alarming trend of dramatic increases in cyber incidents every year. Whether the consequence for unlawful cyber activity be prosecution, a countered cyberattack, denial of access, or a formal military response, the recommended alternative must provide measures that will deter unlawful cyber activity enough to generate a sizeable decrease in the amount of cyber intrusions and attacks.

Alternatives

The problem of accountability in cyberspace has a number of potential solutions. This paper will discuss three. None provide for an immediate remedy to the accountability issue in cyberspace, but instead, will take years to fully develop. The recommended alternative, however, will provide for the ability to prioritize initiatives based on the end goal desired with the hope that once institutionalized, the higher level of security and accountability provided makes the reward worth the effort expended to get there. Once in place, these alternatives may provide a stronger deterrent for cyber criminals and cyber attackers as they seek to create a higher level of accountability than currently exists.

Alternative #1 – Strengthen the Tools for Individual State Governance

The first alternative is to continue with individual state cyber governance while pushing for the establishment of extradition treaties, international shared norms, and stronger internal security controls. The successful case with the Estonian cybercrime ring can be used as a model for the development of formal transnational coordination processes and extradition treaties with other nations. Since the extradition treaty was the key component that determined the success of that operation, developing these treaties with other nations could be elevated to a top priority on the strategic agenda. Since many extradition policies require dual criminality, where the crime committed must be considered a crime in both countries, nations could work together to create mutually agreed upon definitions to cyber terms as well as similar thresholds for criminalization of cyber incidents. While the extradition treaty in the case of Estonia was the foundation for its success, the extensive coordination effort between the multiple countries involved was also

lauded and could be used as a model for the development of formalized processes for information sharing, investigation procedures, evidence collection, and criminal prosecution.

The United States could also publish a formal framework for response, particularly for response to state-sponsored cyber incidents, based on its own internally agreed upon definitions of cyber terms. This framework would clearly express the U.S. intent to respond to nefarious cyber activity with proportionate countermeasures. Nations have always remained vague in their paths toward escalation of conflict, most likely to allow flexibility and to avoid disruption of the status quo. However, the purpose of setting these clear expectations on response would be to communicate to other nations that certain acts in cyberspace will have consequences in the hopes that it will serve as a deterrent to make nations more cautious in crossing "the line." If other countries choose to adopt this practice, it can ultimately result in the creation of shared norms within the international community.

Individual state governance is based on the concept of sovereign control within geographically defined borders. Therefore, technological focus could be directed at creating territorial borders in cyberspace based on existing physical borders. At its roots, the environment of cyberspace is man-made, and as such, the creation of territorial borders in cyberspace is completely feasible.[42] Technological focus on improved and mandated source tagging of data would provide for more accurate authentication as information moves through the entry channels of these territorial borders.[43] An analogy that illustrates how this works would be a car moving along a freeway that is required to broadcast its VIN number, license, weight, and other data

[42] Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," Strategic Studies Quarterly 5, no. 1 (Spring 2011): 35.
[43] Ibid, 41

each time it approaches an exit.[44] If the owner of that freeway node does not approve of the authentication information, the car would either be denied access or forced onto a different road.[45]

For this endeavor, China emerges as a surprising example to emulate. It is widely known that China's Internet content is highly regulated by their government. However, many people do not know that they are able to do so through the establishment of three main Internet gateways that connects its one-billion-plus population to the rest of the world.[46] Of course, it is not suggested that similar security controls on Internet content be emulated, but perhaps with mandatory source tagging, high speed cables, filtering servers, centralized gateways, and more, the security of the Internet content entering and leaving the United States could be greatly improved on through the creation of these virtual borders. The example of China reveals that this endeavor is technologically possible. While many may argue that this governance may encroach on individual freedoms, it is important to remind the critics that "physical borders are known, accepted, and desired by citizens in modern civil societies, and that psychological comfort will be no different for the creation of borders in cyberspace."[47]

Alternative #1 - Analysis

This alternative presents a reasonable and achievable end state as it most closely aligns with the current path of the United States. The successful extradition and prosecution of the Estonian cybercrime ring provides evidence that this alternative can be effective in ensuring accountability once the groundwork to establish some key foundational elements has been

[44] Ibid.
[45] Ibid.
[46] Ibid, 42.
[47] Ibid.

accomplished. When evaluated against whether it has the potential to resolve the barriers to regulation presented in this paper, a focused effort to establish extradition treaties with other nations could help to resolve many of the jurisdictional issues that exist, and also would improve foreign relationships due to the high level of cooperation required to develop these treaties. However, if the policy of dual criminality is to continue, the success of this cooperative effort will depend on the ability of the United States and other nations involved to come to a mutual agreement on basic cyber laws and on the definitions of cyber language. This is a task that up until now, has proven to be complex and difficult. This is most likely due to each country having their own strategic agenda that dictates how they define cyber terms and set cyber laws. Without some sort of unbiased moderator to reconcile the differences and ensure the process is fair to every nation, the standardization of terms and laws could remain at an impasse. Even if standardization was to be achieved and extradition treaties are established with every nation, the process of doing so could take many decades as the United States would need to reconcile these elements with every nation that holds a stake in cyberspace. This process has the potential to be taxing of time and resources, and in the meantime, it would allow the prevalence of cyber incidents to grow or continue at the high rate at which it is currently.

While consistency can be achieved by establishing a framework for response to state-sponsored cyber incidents, there would most likely be little consistency when dealing with cyber intruders working independently. Even if every nation was able to enact their own internal cyber laws, differences can still exist between the activities that constitute unlawful behavior. As a result, cyber attackers and criminals may continue to carry out attacks from countries that have more relaxed cyber laws.

Alternative #1 can provide a form of deterrent to potential cyber intruders once it is achieved due to the higher amount of prosecutions generated and the potential consequences to other states sponsoring unlawful cyber activity. However, unless the lengthy process to establish extradition treaties and to standardize terms and laws is expedited, the level of deterrence to create a sizeable decrease in cyber incidents will not be realized for a very long time. Network infrastructure improvements can provide a deterrent, but the United States may find difficulty in influencing the rest of the world to adopt the practices of source tagging and other authentication protocols, just as they have had in influencing other nations to adopt cyber laws. As mentioned earlier, America's stake in improving cyber security is much greater than other nations and as a result, it is more willing to dedicate resources toward this endeavor. Certain countries may also approach U.S. initiatives with skepticism and question ulterior motives. In the meantime, it is also not entirely reasonable to prohibit all data entering the country without a source tag as this could have severe implications for international trade and the economy.

Alternative #2 – State Level Accountability

The second alternative would be for the United States to hold countries accountable for all cyber activity originating within their physical borders. Today, attribution capabilities have advanced far enough to identify the origin of many cyber incidents. However, once the incident is narrowed down to the country of origin, it is sometimes difficult to argue whether the perpetrator acted in an individual capacity or under the sponsorship of the state. Even when forensic evidence points to the responsible organization as sponsored by the state, the state will usually deny the accusation and the situation then reaches a stalemate.[48] Therefore, one solution

[48] House, *Planning for the Future of Cyber Attack: Hearings before the Subcommittee on Technology and Innovation, Committee on Science and Technology*, statement by Robert Knake, 111th Cong., 2nd sess., 2010, 88-98.

would be for the United States to hold the state responsible for all unlawful cyber activity, whether it is state-sponsored or not.

While many cyber-attacks do not rise to the level of an armed attack, they do violate the customary international law norm of nonintervention, or the obligation of a sovereign state to not intervene with another sovereign state.[49] Existing legal frameworks allow for proportionate countermeasures to be carried out in response to wrongful acts committed by another state, and the boundaries of cyberspace should be included within the scope of this internationally recognized law.[50] The previous discussion on developing proportionate countermeasures in Alternative #1 can also be applied in this alternative, but on a more universal scale as the countermeasures would not only apply in the case of state-sponsored cyber incidents, but also in the case of incidents that are not sponsored by the state.

While the law of nonintervention and the law of countermeasures have traditionally applied to state-sponsored cyberattacks, it could be further argued that a sovereign state has an inherent responsibility to ensure that their network infrastructure and legal frameworks sufficiently provide a certain level of accountability and security so that their borders do not become a breeding ground for criminal cyber activity. The United States does not condone the physical harboring of terrorists by other countries and this sentiment could be extended and more clearly expressed to apply to activities in cyberspace. Drawing on Michael Sheehan, former U.S. Ambassador at Large for Counterterrorism, and his message to the Taliban's foreign secretary in 1999 regarding Al Qaeda attacks, "If you have an arsonist in your basement, and every night he

[49] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegal, "The Law of Cyber-Attack," Faculty Scholarship Series, Paper 3852, January 2012.
[50] NATO Cooperative Cyber Defence Centre of Excellence, Talinn Manual, 36.

goes out and burns down a neighbor's house, and you know this is going on, then you can't claim you aren't responsible."[51]

Similar to Alternative #1, this alternative will also require policy makers in the United States to internally agree on an accepted set of definitions for the various cyber terms. These definitions could be published to the international community and used by the United States to determine appropriate countermeasures for violations. However, in this alternative, the United States would apply proportionate countermeasures to the violating state, rather than to the individual committing the unlawful act. The violating state would then have the prerogative to investigate and prosecute the individual. By holding states accountable, much of the ambiguity in identifying whether a cyber incident can be attributed to a state or an individual is eliminated. This frees up national leaders and policy makers to focus more heavily on what to do about the unlawful activity rather expending resources on advanced attribution capabilities to find out who, individually, is responsible.

Alternative #2 – Analysis

Alternative #2 would resolve all the barriers to regulation discussed. The benefit of this alternative is that it requires only that the United States comes to internal agreement, rather than international agreement, on accepted definitions to cyber terms and the activities that constitute unlawful behavior for each of these terms. Once this is established, jurisdictional issues no longer become an issue since a published framework for response calls for some sort of consequence to be applied to a violating state rather than an individual. Accurate attribution capabilities become more important in order to determine the state to be held responsible. With

[51] House, *Planning for the Future of Cyber Attack*, 95.

clearly defined thresholds for conflict escalation, foreign relationships may be improved through clear communication of expectations.

This alternative also provides for a consistent approach to accountability. Developing proportionate consequences to the varying degrees of malicious cyber activity sets standard responses to be expected by violating states. It will also exude an appearance of fairness as all nations are treated equally.

This alternative will also provide a significant deterrent for potential cyber intrusions. First, states will be more likely to establish cyber laws to help ensure cyber attackers and cyber criminals within their borders do not violate the cyber laws of the United States and escalate tensions or trigger devastating consequences. Second, in making the international community aware of what constitutes unlawful cyber activity in the United States and the consequences for carrying out such activities, certain nations may be more likely to take some such risky actions "off the table."[52] The Cuban Missile Crisis in 1962 provides a good lesson that illustrates this point, as it was the result of the United States and the Soviet Union failing to clearly define their thresholds regarding nuclear weapons and the paths to escalation. With the U.S. putting missiles into Turkey and the Soviets into Cuba, the level of tension was unintentionally raised and provoked reactions beyond each country's expectations.[53] The quickly escalated actions between the two nations almost brought on a thermonuclear war.

The final criteria for evaluating Alternative #2 is whether the solution is practical. While this alternative has successfully met all other criteria, it is not entirely practical to hold an entire state accountable for all cyber activity, especially from those groups or individuals acting

[52] Lieberthal, *Cybersecurity and U.S.-China Relations*, X.
[53] Ibid, 29-30.

independently. Doing so could invoke unintended consequences such as turning the cyber environment in many states into radical, authoritarian regimes where users are under constant surveillance and heavily punished for misdemeanor cybercrimes in an effort to avoid escalation of conflict. As cyber security specialist Robert Knake warns, "Indeed, a world in which states monitor and constrain citizen activities to prevent crimes before they take place would be a very frightening world."[54]

Alternative #3 – International Body for Cyberspace Governance

The third alternative is to focus efforts and resources toward the creation of an international body for cyberspace governance. Many of the problems with accountability in cyberspace transcend national borders. The increasing prevalence of cyber incidents reveal that it is not a problem that a single country, or even a few, can tackle on its own given unlimited resources. It is a problem that will require the participation of every nation in order to overcome. However, the United States, in its efforts to establish accountability in cyberspace, has found that every nation has their own strategic agenda that does not necessarily align with that of the United States. A collaborative forum would require states to move beyond their individual agendas and work together to create one strategic agenda for the governance of cyberspace as a whole. While there are organizations currently dedicated to multi-national collaboration, such as the Council of Europe's Convention on Cybercrime, their scopes are either too narrow, their power too limited, or they are too exclusive in the extent of their memberships. An international body for cyberspace governance could address accountability for all types of malicious cyber activity, involve the entire international community, and have the ability to invoke consequences against

[54] House, *Planning for the Future of Cyber Attack*, 95.

nations that do not abide by the basic laws set forth, similar to the way the United Nations votes to impose sanctions on nations that threaten peace. While obtaining buy-in from all countries will take some time, the United States and its major allies could take the lead in the initial establishment of an organization to address cyberspace issues. As standard protocols are developed and enforced, more nations will have an incentive to participate.

An international body could work to resolve issues pertaining to standardization of cyber language, cyber laws, and network protocols. By employing information technology leaders representing a multitude of member states, the dedicated effort to overcome standardization issues has the potential to expedite the process of achieving universally accepted terms and laws that would govern behavior in cyberspace. Of course, individual states would still have the power to enact stricter controls, but the establishment of basic laws that govern acceptable rules to protect the freedom and security of internet users would be the main goal of this organization.

In addition, a team of international experts could focus on the standardization of network protocols that would establish shared norms for information technology practices. One area that would require attention is the unregulated arena of Internet Service Providers (ISP). ISPs technically have the ability to track all malicious activity on their networks along with the points of origin of this activity.[55] However, they are not required to track this information.[56] An international body could mandate and ensure worldwide compliance of ISPs to track and store this information to aid in cyber investigations. An international body could also ensure source tagging and other certain authentication protocols become the international standard. Failure to

[55] Ibid.
[56] Ibid.

accept or adhere to these international standards would mean limited connection to the vast array of services that cyberspace affords through closure of certain gateways to unauthenticated data.

The organization could also employ within its structure cyber forensics specialists and investigative teams for the purposes of attribution, evidence collection, and potentially, prosecution. This will require the organization to possess some form of universal jurisdiction to overcome the obstacles presented with jurisdictional issues discussed earlier. Once proper attribution and investigation is accomplished, the organization may have the ability to determine whether the perpetrators shall be prosecuted within the country where the attack originated, within the victim state, or within an international court of law. This determination could be based on the extent of cyber effects generated.

Alternative #3 – Analysis

Similar to Alternative #2, Alternative #3 also has the potential to fully resolve all the barriers to regulation presented in this paper. While the barriers may not be as easily resolved as in Alternative #2 due to the international effort required, this alternative presents an easier challenge when compared to Alternative #1. The collaborative forum that this alternative provides has the potential to expedite the resolution of standardization issues through the creation of one strategic agenda that can eventually result in one set of definitions for cyber terms and a universal set of basic laws that govern cyberspace as a whole. The establishment of universal jurisdiction would help to resolve the jurisdictional issues that exist by allowing for the extradition of cyber criminals and cyber attackers to be prosecuted. A governing body also has the potential to improve foreign relationships as it presents more of an impartial moderator to reconcile the multitude of issues pertaining to cyberspace. However, for states that do not

comply with the international body's policies, this alternative then opens up discussion on the economic implications and tensions that may ensue.

This alternative is also practical. Many will argue that an international body that controls the operations of cyberspace will take autonomy away from individual states and will eventually become a surveillance tool that eliminates user privacy. It then becomes important to note that this international body should not be responsible for the constant surveillance of the activities of all internet users. While there is a desire to hold accountable those persons or groups responsible for malicious activity, the intent is not to do so through constant monitoring or through the regulation of Internet content. Rather, the creation of this body would be for the purpose of expediting the establishment of shared norms for conduct in cyberspace and to enact "improvements to the general hygiene of the Internet ecosystem."[57] This alternative recognizes the need for the world to move beyond the belief that anonymity equates to privacy, and further, seeks to create an environment where privacy is achieved through technical means and legal requirements.[58]

This alternative does provide consistency in its approach to accountability due to the creation of a single set of basic laws that govern cyberspace that is based on a universally accepted set of definitions for cyber terms. Since all nations must abide by these laws or face limited access to cyberspace, the incentive to comply is high. A governing body also will ensure fair and equal consequences are carried out against violating states or violating individuals.

Finally, Alternative #3 serves as a deterrent in that it provides for a dedicated organization and system for handling the inordinate amount of problems and issues that have

[57] Ibid, 98.
[58] Ibid.

arisen since the emergence of cyberspace as an operational environment. As the lead agency for tackling the world's most pressing cyber concerns, the combined effects of setting and enforcing standard network protocols, leading international cyber investigations, and carrying out appropriate consequences can potentially be a deterrent for potential cyber attackers and cyber criminals.

Results of Analysis

Based on the analyses of the alternatives, Alternative #3 presents the best option for addressing issues with accountability in cyberspace. The creation of an international body for cyberspace governance has the highest potential for overcoming the obstacles to cyber accountability due to its ability to resolve some of the major barriers to regulation, and its ability to provide for a fair and consistent approach. The alternative is reasonable and can provide a significant deterrent to potential cyber attackers and cyber criminals. While Alternative #1 may be an enticing choice as it also resolves the major barriers to regulation, the extensive amount of time required to achieve the desired outcome may be too long and in the end, does not provide enough consistency to produce a long term solution to the accountability issues. Alternative #2 is the simplest of the three alternatives to achieve and meets almost all the criteria. However, this alternative is not practical due to the extreme nature of the potential unintended consequences.

Recommendation

The United States and its allies should push for the creation of an international body for cyberspace governance. Rather than relying on countries to sign a commitment to establish

legislation like the Council of Europe's Convention on Cybercrime, this body should be the entity actually establishing the policies and regulations that will govern this virtual environment. The most important aspect of Alternative #3 is that it views cyberspace as a whole, rather than from the perspectives of individual states, each with their own strategic agenda. To resolve the problems with accountability in cyberspace, nations will need to move past their myopic views that address only the cyber issues presented within their physical borders. Alternative #3 calls for the world's leaders and subject matter experts to come together for the establishment of one strategic agenda for cyberspace that seeks to create shared norms for conduct and international standards for network protocols.

Conclusion

While the creation of an international body for cyberspace governance is not without its flaws and will likely generate its own set of unintended consequences, it presents the best option for addressing not only the issues with accountability, but also many other issues affecting operations in cyberspace. Problems encountered in cyberspace are rarely isolated to a single country. An international body will have the ability to track issues on a global scale and prioritize initiatives. Of course, the complex nature of international politics will guarantee that tensions will arise, particularly with those countries that are not cooperative of this international effort. In this case, the international body and the nations involved will need to evaluate and balance economic endeavors with maintaining the security of internet users and the channels that allow these economic endeavors to occur. Regardless, any solution to the issue will require a harsher stance to accountability than currently exists.

The intent of this research paper is not to fully resolve the issues pertaining to accountability in cyberspace, but rather, to provide operational direction and open up discussion for further research. The statistics on cyber incidents and the strategic direction from the NSS to hold those accountable for unlawful activity in cyberspace fuels the need to do so. Over a decade ago, it was viewed as a success when organizations were able to identify that their networks were being attacked.[59] Within the last decade, the U.S. government, in conjunction with a multitude of private companies that emerged, have become extremely successful in tracking IP addresses to identify who is responsible.[60] "Now, we can often tell when the networks are being breached and are able to determine who is doing it. So the question now becomes as we move forward in this, is what are we going to do about it."[61]

[59] United States Senate, *Investigating and Prosecuting 21st Century Cyber Threat, 30.*
[60] Ibid.
[61] Ibid.

Bibliography

Alexander, Gen Keith. "U.S. Cybersecurity Policy and the Role of U.S. Cybercom." Discussion (Transcript). Center for Strategic and International Studies, Washington DC, 3 June 2010. Available at: http://www.csis.org/files/attachments/100603csis-alexander.pdf

Archick, Kristin. *Cybercrime: The Council of Europe Convention*. Order Code RS21208. Washington, DC: Congressional Research Service, 2004.

Center for Strategic and International Studies. Net Losses: Estimating the Global Cost of Cybercrime. Staff Study, June 2014.

Clapper, James R. *Worldwide Threat Assessment of the US Intelligence Community*. Washington DC: Senate Select Committee on Intelligence, 2013.

Clapper, James R. *Worldwide Threat Assessment of the US Intelligence Community*. Washington DC: Senate Select Committee on Intelligence, 2014.

Council of Europe, "Convention on Cybercrime: Chart of signatures and ratifications of Treaty 185," Council of Europe, updated 1/26/2016, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

Council of Europe. "European Treaty Series - No. 185." Convention on Cybercrime, 2001, Budapest, 23.XI.2001.

Demchak, Chris C. and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32-61.

Department of Homeland Security, "Critical Infrastructure Sectors," http://www.dhs.gov/critical-infrastructure-sectors.

Finklea, Kristin M. *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Concerning U.S. Law Enforcement*. CRS Report for Congress. Congressional Research Service, January 2013.

Finklea, Kristin and Catherine A. Theohary. *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement.* CRS Report for Congress. Congressional Research Service, January 2015.

Garris, John. "There's No Going It Alone: Disrupting Major Crime Rings (A Case Study)." Bethesda, MD: SANS Institute, 2015.

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegal. “The Law of Cyber-Attack.” *Faculty Scholarship Series*, Paper 3852, January 2012.

House. *Planning for the Future of Cyber Attack: Hearings before the Subcommittee on Technology and Innovation, Committee on Science and Technology.* Statement by Robert Knake. 111th Cong., 2nd sess., 2010.

Hosenball, Mark. “U.S. counterintelligence chief skeptical China has curbed spying on U.S.” *Reuters*, 18 November 2015. http://www.reuters.com/article/us-usa-cybersecurity-idUSKCN0T72XG20151119.

Internet Crime Complaint Center. *2010 Internet Crime Report*. National White Collar Crime Center, 2011.

Internet Crime Complaint Center. *2014 Internet Crime Report*. National White Collar Crime Center, 2014.

The IP Commission. *The Report of the Commission on the Theft of American Intellectual Property*. The National Bureau of Asian Research, May 2013.

Lieberthal, Kenneth and Peter W. Singer. *Cybersecurity and U.S.-China Relations.* Washington, D.C.: The Brookings Institution, February 2012.

Menn, Joseph. “Cyber Attacks Against Banks More Severe Than Most Realize,” *Reuters*, 18 May 2013. http://www.reuters.com/article/us-cyber-summit-banks-idUSBRE94G0ZP20130518.

Morrison, Wayne M. *China-U.S. Trade Issues*, CRS Report for Congress RL33536. Washington DC: Congressional Research Service, 2015.

NATO Cooperative Cyber Defence Centre of Excellence. “Cyber Definitions.” https://ccdcoe.org/cyber-definitions.html.

NATO Cooperative Cyber Defence Centre of Excellence. *Talinn Manual on the International Law Applicable to Cyber Warfare*, 2013.

Obama, Barack H. *National Security Strategy*. Washington, D.C.: Government Printing Office, 2010.

Obama, Barack H. *National Security Strategy*. Washington, D.C.: Government Printing Office, 2015.

Obama, Barack H. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, D.C.: The White House, May 2011.

Prasad, Krishna. “Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework.” Paper presented at the 3rd Australian Counter Terrorism Conference. Perth, Australia, 3-5 December 2013.

Senate. *Investigating and Prosecuting 21st Century Cyber Threats: Hearings before the Subcommittee on Crime, Terrorism, Homeland Security and Investigations*. 113th Cong., 1st sess., 2013.

Shelton, Gen William L. Speech. AFCEA Cyberspace Symposium, Colorado Springs, CO, 6 Feb 2013.

Speer, David L. “Redefining Borders: The Challenges of Cybercrime.” *Crime, Law and Social Change* 34, no. 3 (October 2000): 259-273.

United States Faces Challenges in Addressing Global Cybersecurity and Governance. Washington DC: U.S. Government Accountability Office, July 2010.

Waddell, William, David Smith, James Shufelt, and Jeffrey Caton, United States Army War College. Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace, CSL Study 1-11, Center for Strategic Leadership, March 2011.

Wilshusen, Gregory C. *Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges*. Washington D.C.: U.S. Government Accountability Office, 2013.